specialized training as specified in DoD Directive (DoDD) 8570.1, "Information Assurance Training, Certification, and Workforce Management" of Aug. 15, 2004, and its associated manual, DoD 8570.01-M, "Information Assurance Workforce Improvement Program."

DON compliance with FISMA requirements ensures that the Department performs due diligence in practicing information assurance, as well as in gathering and reporting data on the security status of its IT systems and networks.

For further information, refer to these previously published FISMA articles available at the *CHIPS* Web links given below.

"The Federal Information Security Management Act of 2002" – http://www.chips.navy.mil/archives/04_winter/Web_Pages/FISMA.htm.

"FISMA Update" – http://www.chips.navy.mil/archives/05_OCT_DEC/web_pages/FISMA.htm.

Jim Collins is a member of the DON CIO Information Assurance Team. CHIPS

Sailors Warned of VA Data Compromise

From Chief of Naval Personnel Public Affairs

The Department of Veterans Affairs (VA) announced June 3 that active-duty Sailors may be affected by the theft in May of military personnel data. According to the VA, a duplicate database with data files was stolen from a VA employee's home May 3. While the VA has received no reports that the stolen data has been used for fraudulent purposes, they are asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions.

Several resources are available for people to go to for more information. The Department of Veterans Affairs has set up a special Web site (www.firstgov.gov) and a toll-free telephone number (800-FED-INFO or 800-333-4636) that feature up-to-date news and information on the data compromise.

The site offers tips on how to check credit reports, how to guard against identity theft and whom to call if an individual believes any fraudulent activity is occurring using his or her personal information.

The Navy and Department of Defense are working closely with the VA to determine how many Sailors and other service members may be affected by the compromise of records. Sailors whose information has been compromised will be notified by a letter from the VA and the Navy so they can take the appropriate steps.

Tips on how to watch for suspicious activity include the following:

√ Closely monitor your bank and credit card statements for fraudulent transactions. Monitoring accounts online is the best way to detect fraud early.

√ Place a 90-day fraud alert on your credit report, which tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. This action may cause some delays if you are trying to obtain new credit.

It is only necessary to contact one of the three companies below to place an alert. That company is then required to contact the other two.

The companies are Equifax (800-525-6285, www.equifax.com); Experian (888-397-3742, www.experian.com); and TransUnion (800-680-7289, www.transunion.com).

Once the fraud alert has been posted, you are entitled to free copies of your credit reports. Review these reports for inquiries from companies you haven't contacted or accounts you didn't open. The alert can be renewed after 90 days. Sailors are advised to take the following steps if they discover fraudulent accounts or transactions:

√ Contact the financial institution to close the fraudulent account(s) that have been tampered with.

√ File a report with the local police department.

√ File a complaint with the Federal Trade Commission by phone at 877-438-4338, online at www.consumer.gov/idtheft or by mailing a letter to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C., 20580.

Other Web sites with more information on how to guard against identity theft include:

www.privacy.ca.gov/sheets/cis3_english.htm
www.co.boulder.co.us/da/consumer/idtheft.htm

For more news from around the fleet, visit Navy NewsStand at www.navy.mil. CHIPS

CHIPS Article Guidelines

CHIPS welcomes articles from our readers. Please submit articles via e-mail as Microsoft Word or text file attachments to chips@navy.mil. To discuss your article with a CHIPS editor, call (757) 444-8704 or DSN 564-8704. Go to the CHIPS Web site at http://www.chips.navy.mil/chipsguidelines.html for more information.